MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

DISSERTAÇÃO

FRAMEWORK DE AUTO-AVALIAÇÃO INTERNA PARA GESTÃO DA SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO

JOÃO NUNO ESTEVES PINA

SETEMBRO - 2012

MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

DISSERTAÇÃO

FRAMEWORK DE AUTO-AVALIAÇÃO INTERNA PARA GESTÃO DA SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO

JOÃO NUNO ESTEVES PINA

ORIENTAÇÃO:

PROF. DOUTOR MÁRIO CALDEIRA (ISEG-UTL)

MESTRE ARMINDO MACEDO (ISEG-UTL)

SETEMBRO - 2012

Índice

A - Índice de Figuras

B - Índice de Tabelas

C - Lista de Acrónimos

DRH	Direcção de Recursos Humanos
DRP	Direcção de Recursos Patrimoniais
DSTIC	Direcção de Serviços de Tecnologias de Informação e Comunicações
ENISA	*European Network and Information Security Agency* - Agência Europeia para a Segurança das Redes e Informação
ISMS	*Information Security Management System*
ISO/IEC	*International Organization for Standardization/International Electrotechnical Commission*
MOPTC-SG	Ministério das Obras Publicas Transportes e Comunicações – Secretaria - Geral
PDCA	*Plan–Do–Check–Act*
SGMOPTC	Secretaria - Geral do Ministério das Obras Publicas Transportes e Comunicações
SGSI	Sistema de Gestão da Segurança da Informação
SITI	Sistemas e Tecnologias da Informação

D – Agradecimentos

Ao Salvador, Patrícia, aos meus pais, e a todos aqueles

que contribuíram de alguma forma para a realização deste trabalho.

FRAMEWORK DE AUTO-AVALIAÇÃO INTERNA PARA GESTÃO DA SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO

João Pina – ISEG/UTL – Mestrado em Gestão de Sistemas de Informação

Resumo

A importância da protecção da informação, associada aos factores de insucesso na implementação de Sistemas de Gestão da Segurança da Informação (SGSI), cria a necessidade de adoptar modelos de planeamento de segurança cada vez mais eficazes nas organizações. Um SGSI pretende garantir a utilização das boas práticas de gestão da segurança da informação, bem como a utilização de mecanismos que maximizem a eficácia dos seus sistemas de informação. Neste sentido, e face aos factores de insucesso verificados na literatura, e aos modelos estudados ao longo da revisão bibliográfica, o principal objectivo deste estudo foi o de procurar analisar o contributo de um mecanismo de auto-avaliação interna prévia na implementação de um SGSI numa organização. O estudo de caso do Ministério das Obras Publicas Transportes e Comunicações – Secretaria-Geral (MOPTC-SG), apresenta um procedimento de auto-avaliação interna com base nos controlos (ISO/IEC 27002:2005, 2005), aferindo o grau de conformidade do organismo, níveis de performance, níveis de exposição e vulnerabilidade, procedimentos de consciencialização e responsabilização. Os resultados parecem indicar que a utilização destes processos, além de complementar os modelos existentes, permite um conhecimento mais abrangente, consciente, eficaz e antecipado do risco, garantindo à organização uma implementação e utilização mais eficiente dos seus SGSI.

Palavras chave: *Information Security Management System*, ISO/IEC 27002:2005, auto-avaliação.

SELF- EVALUATION FRAMEWORK FOR INTERNAL MANAGEMENT OF INFORMATION SECURITY: A CASE STUDY

João Pina – ISEG/UTL – Master of Management Information Systems

Abstract

The importance of information protection, associated with factors that may influence the failure of Information Security Management Systems (ISMS) implementation, create the need for more effective security planning models in organizations. An ISMS seeks to ensure the use of good information security management practices, as well as the use of mechanisms that maximize the effectiveness of existing information systems. In this line of thought, given some failure factors observed in the literature, and the models studied throughout the literature review, the main goal of this study was to analyze the possible contribution of an internal self-assessment mechanism prior to the implementation of an ISMS in an organization. The case study of the Secretary-General of the Ministry of Public Works Transport and Communication (MOPTC-SG), presents on such internal self-assessment based on industry standard controls (ISO / IEC 27002:2005, 2005). This set of controls represent a framework that measures the degree of organization compliance, levels of performance, levels of exposure and vulnerability, awareness and accountability procedures. The results seem to show that by using these processes, complemented by existing models, a more comprehensive knowledge, awareness, and early risk assessment a more efficient implementation can be achieved.

Keywords: Information Security Management System, ISO/IEC 27002:2005, self – evaluation.

1. Introdução

1.1.Enquadramento

No contexto actual de competição e exigência empresarial cada vez mais eficaz entre organizações, a importância das Tecnologias da Informação (TI) e respectivos suportes por parte das empresas e organismos, é encarada cada vez mais como uma vantagem competitiva dentro da área do conhecimento do negócio, (Serrano, et al., 2004), não sendo possível analisar as oportunidades e ameaças organizacionais sem este conhecimento (Earl & Feeny, 2000).

Esse conhecimento e a sua consequente protecção, surge como um activo importante para o negócio e de valor para a organização, sendo que esse valor de negócio precisa de ser protegido apropriadamente (ISO/IEC 27000:2009, 2009).

A importância dessa informação e a dependência dos organismos dos Sistemas e Tecnologias da Informação (SITI) é cada vez mais relevante, ou seja, segundo Earl & Feeny (2000) as oportunidades e ameaças organizacionais têm de ser analisadas conjuntamente com esse conhecimento, assumindo os SITI um papel cada vez mais estratégico na tomada de decisão dentro das organizações.

O uso das ferramentas adequadas de apoio à gestão, e respectiva tomada de decisão no sentido de optimizar os níveis de desempenho e eficácia nas organizações, é referido por Macedo (2009), que salienta a importância da definição objectiva dos recursos, funções e contributos, dando a cada entidade e/ou pessoa a noção de localização, função e contributo para a estratégia e missão da organização.

Calder & Watkins (2008) referenciam ainda, que numa era caracterizada pela importância da informação e da economia da informação, identificada por mercados, recursos, informação e conhecimento globalizado, é cada vez mais premente a adopção de ferramentas e das boas práticas de Governança TI, no sentido de lidar com esta realidade actual.

Neste sentido, Dhillon (2006), menciona ser impossível garantir essa protecção sem a utilização de *standards*, possibilitando aferir níveis de segurança e verificar níveis de performance (CGTF, 2004). Por outro lado, Straub & Welke (1998), constataram que os profissionais, internos à organização, estão dispostos e aptos a usar as necessárias *frameworks para* o respectivo planeamento da segurança da informação.

Neste caso, a importância do planeamento da segurança através de ferramentas teóricas ou *frameworks,* e a formalização desses procedimentos, como demonstra Straub & Welke (1998), garantem capacidade à organização de se organizar, optimizar e alocar recursos em áreas identificadas previamente como criticas ou deficitárias, em termos de segurança da informação.

Desta forma, a implementação de um SGSI nas organizações pretende garantir as boas práticas de gestão de segurança da informação nas organizações, (ISO/IEC 27000:2009, 2009), ou simplesmente como refere CGTF (2004), a utilização de guias das boas práticas de segurança como a ISO/IEC 27002:2005 (2005), permitindo medir a performance da segurança da informação nas organizações.

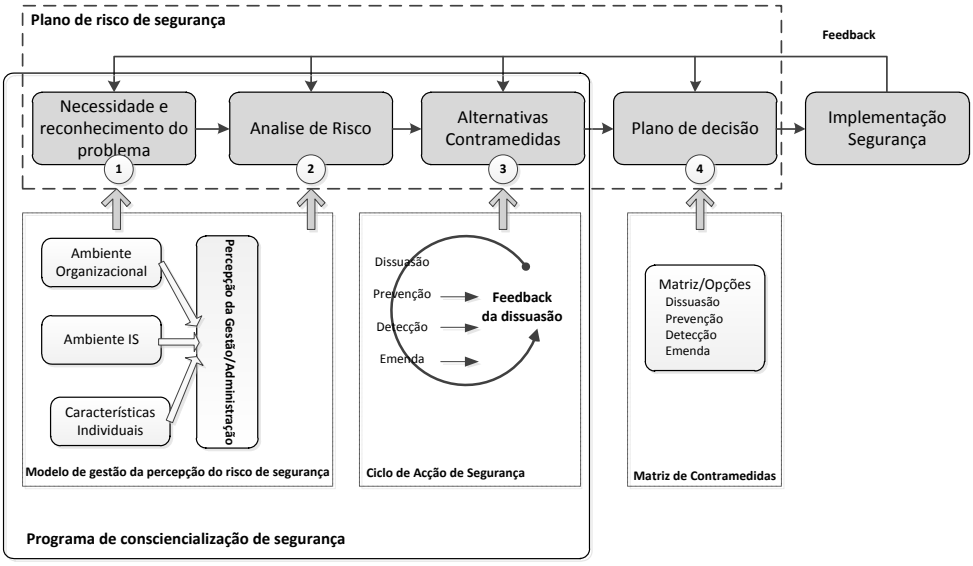
Conforme estabelecido no *standard* ISO/IEC 27001:2005 (2005), e abordado por Calder & Watkins (2008), existem factores chave para o estabelecimento de um ISMS (*Information Security Management System*) e consequentemente para o sucesso da sua implementação. A

importância da definição de uma política de segurança, a definição prévia dos objectivos base e de um âmbito claro e conciso do ISMS a implementar, é um requisito basilar para o sucesso da implementação, e do estabelecimento de uma política de gestão da segurança na organização.

Além destes a experiência demonstra, de acordo com os inúmeros projectos de certificação já realizados, referindo ISO/IEC 27002:2005 (2005), que muitos dos factores associados ao insucesso de implementações, passam essencialmente por uma falta de conhecimento prévio da organização sobre os seus sistemas e segurança da informação, indefinição de políticas de segurança, falta de definição e alinhamento de objectivos com a organização, bem como algum défice de envolvimento da organização em todo este processo. Facto, que pode ser acautelado com processos de avaliação interna prévios como forma de preparar, consciencializar e resolver não conformidades como menciona CGTF (2004), ou Straub & Welke (1998) na capacidade interna das organizações de realizarem o seu respectivo planeamento de segurança.

Estes processos de avaliação prévia, podem ser estabelecidos através de avaliações internas nas organizações, utilizando de facto, como referido anteriormente, os controlos inscritos no *standard* (ISO/IEC 27002:2005, 2005) como ferramentas de avaliação da organização e uso das boas práticas. Pretende-se desta forma, estabelecer mecanismos que promovam o envolvimento e conhecimento dentro da organização, (Straub & Welke, 1998), que garantam conhecimento interno e auxiliem a implementação de um ISMS. Torna-se portanto necessário, estabelecer um modelo que permita mitigar as falhas comuns de implementações ineficazes de SGSI, processos mal conduzidos, falhas de planeamento, bem como perspectivas e expectativas goradas que descredibilizam a implementação destes sistemas.

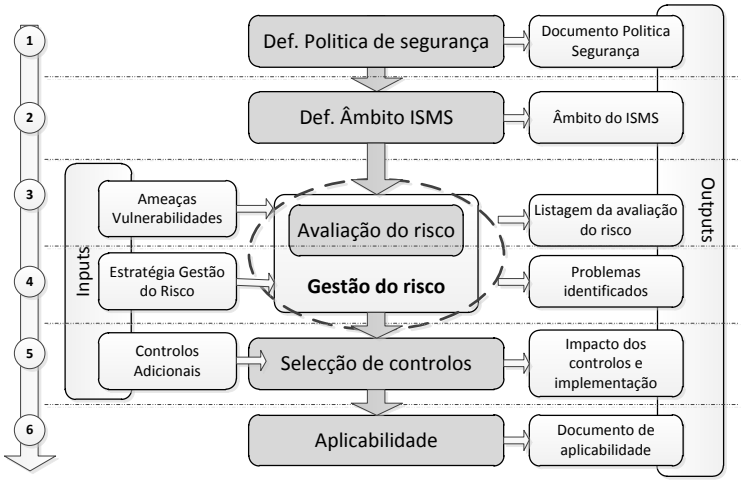
Na *framework* de planeamento do risco de segurança de Straub & Welke (1998), conforme Figura 1-1, os autores apresentam um claro envolvimento da organização em todo o processo de gestão da segurança, assinalados em cinco grandes passos: reconhecimento do problema; análise de risco; alternativas e contramedidas; plano de decisão; implementação. Dentro do plano do risco da segurança, salienta-se a importância do reconhecimento do problema e de um âmbito claro associado, com um plano cíclico e realimentado com melhorias identificadas, aumentando assim, gradualmente os seus níveis de eficácia. Outro importante bloco a salientar, é o programa de consciencialização de segurança, constituído por um modelo de percepção do risco de segurança, onde avalia o ambiente organizacional, e um ciclo de acção de segurança onde se introduzem contramedidas e planos de dissuasão do problema. Por outro lado, salienta-se também no plano de decisão, a matriz de contramedidas, que analisa e gera opções de decisão em todo o processo de implementação da segurança (plano de risco de segurança).



Fonte: Adaptado de Straub&Welke (1998)

Figura 1-1 *Framework* Straub & Welke(1998)

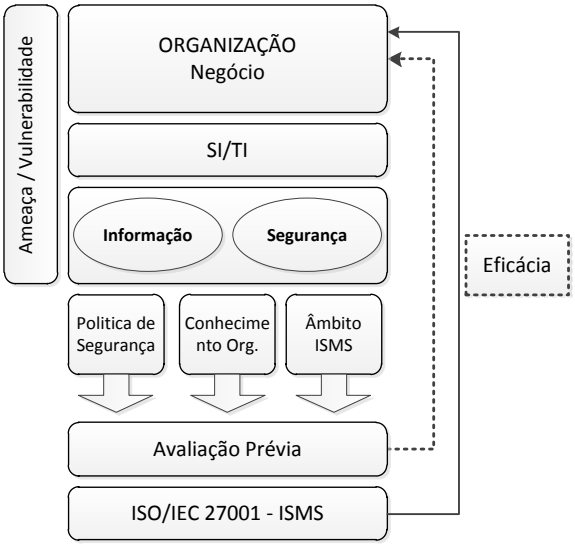
Por outro lado, a *framework* ISMS, (ENISA, 2012), pretende estabelecer métodos e ferramentas que promovam a resolução dos problemas, associados ao fraco conhecimento das actividades de gestão de risco nas organizações, à ausência de uma "linguagem comum" na área de gestão de risco que facilite a comunicação entre as partes interessadas, à falta de conhecimento, casos de estudo, ferramentas e boas práticas, além da necessidade de avaliar a interoperabilidade de métodos e a sua integração com a área de governança corporativa. A *framework* proposta, Figura 1-2 *Framework* ISMS da ENISA, surge na sequência de um guia de propostas definindo para o efeito 6 passos orientadores: Definição da política de segurança; Âmbito do ISMS; Avaliação do risco; Gestão do risco; Selecção de controlos e aplicabilidade. Toda a *framework* atribui especial atenção aos necessários *inputs* e *outputs* com especial foco no passo 3 e 4, onde se efectua uma avaliação e gestão do risco, e onde se salienta a importância da estratégia e a definição de controlos, para que o processo de gestão e avaliação reproduza uma implementação mais consistente com identificação dos riscos e das fraquezas.



Fonte: Adaptado de ENISA (2012)

Figura 1-2 *Framework* ISMS da ENISA

Com base na teoria de planeamento de segurança, (Straub & Welke, 1998), e na *framework* ISMS, (ENISA, 2012), é proposto um novo modelo conceptual ao longo do trabalho, que pretende identificar conceitos e variáveis, que descrevam a sequência lógica de análise subjacente à implementação de um ISMS. Neste novo modelo, Figura 1-3 Modelo conceptual, destacam-se o alinhamento da organização com o negócio num primeiro passo, associado a toda a componente SITI, como referido por Earl & Feeny (2000). Este passo interliga a dois grandes grupos, informação e segurança, sendo que será a partir destes que se deverá extrair toda a componente de conhecimento, política de segurança e âmbito do ISMS a implementar, conforme ENISA (2012). É proposto neste estudo, e com base nas referências anteriores, integrar um novo passo no modelo proposto de Avaliação Prévia da organização, gerando este informação estratégica em termos de decisão para a organização, como proposto por ISO/IEC 27002:2005 (2005) e Straub & Welke (1998). Pretende-se garantir uma maior eficácia para o passo seguinte de implementação efectiva do ISMS com a consolidação desta avaliação. Neste novo modelo é ajustado o passo 5 do modelo ISMS da ENISA (selecção de controlos),Figura 1-2 *Framework* ISMS da ENISA, para um cenário de Avaliação Prévia com controlos ISO/IEC 27002:2005 (2005), que garanta e maximize os níveis de eficácia na implementação ISMS, bem como garantir os necessários *inputs* à gestão/organização. Nesta fase intermédia (Avaliação Prévia), é utilizada uma nova *framework* de avaliação da segurança da informação maximizando a eficácia da implementação do ISMS. Por outro lado é usada a componente conhecimento da organização da mesma forma que Straub & Welke (1998) utiliza no seu programa de consciencialização de segurança, introduzindo a necessidade de conhecimento, percepção do problema e introdução de alternativas para a eficácia do plano de risco de segurança.



Fonte: Adaptado de (Straub&Welke, 1998) e *(ENISA, 2012)*

Figura 1-3 Modelo conceptual

Esta *framework* que utiliza os controlos ISO/IEC 27002:2005 (2005), consubstanciada no passo intermédio Avaliação Prévia do modelo conceptual, é testada e apresentada como estudo de caso no âmbito do MOPTC-SG. Os resultados foram utilizados ao longo do modelo estabelecido, quer em termos de maximização dos níveis de eficácia na implementação de um ISMS, quer como garantia de *inputs* à gestão/organização no apoio à tomada de decisão.

Pretende-se demonstrar através do estudo de caso apresentado, e como refere Straub & Welke (1998), que as organizações devem usar os controlos mais eficazes para conhecimento interno (auto-avaliação), e controlo do risco de segurança, usando as suas *frameworks* para o seu respectivo planeamento de gestão da segurança, obedecendo a *standards* (Dhillon, 2006).

A bibliografia aponta que a criticidade do tema associado à segurança da informação, bem como a relevância científica do problema associado à falta de ferramentas de avaliação, é notória, Calder & Watkins (2008), tendo em conta o desconhecimento das actividades de

gestão de risco nas organizações, existindo para o efeito vários trabalhos de investigação científica na área, que promovem a optimização de modelos e ferramentas, com vista a optimizar planos e procedimentos de gestão do risco. Durante a implementação de um SGSI, são identificadas frequentemente falhas de implementação, que condenam à partida o sucesso do projecto e os seus principais objectivos, sendo que associado a este problema podemos identificar outros resultantes também do desconhecimento das ameaças internas e externas, a que a organização se encontra exposta. A importância e consciência da situação da organização, aliada à importância da antecipação do risco, com identificação prévia dos seus pontos de falha, vulnerabilidades ou níveis de exposição, garantem a pertinência da realização de uma auto-avaliação, através da utilização das boas práticas e *standards* de segurança da informação.

Neste sentido, é apresentado de forma sumária o objecto de investigação, que se consubstancia no estudo de caso do MOPTC-SG, e onde se analisa o contributo de uma auto-avaliação interna prévia na implementação de um SGSI. Para a realização deste trabalho, para além da revisão bibliográfica, é efectuado o enquadramento teórico da norma ISO/IEC 27000, além da referida descrição do estudo de caso, com a apresentação dos resultados obtidos no âmbito da validação dos controlos realizada.

1.2.Questão de investigação

Para o efeito, e com base nos problemas identificados ao longo da revisão da literatura, e no estudo de caso apresentado, surge a seguinte questão de investigação: Qual o contributo de um processo de auto-avaliação interna prévio ISO27002, na implementação de um Sistema de Gestão da Segurança da Informação?

1.3.Segurança da Informação

Como descrito na ISO/IEC 27000:2009 (2009), a informação é um activo que como outros activos importantes para o negócio tem valor para a organização, e por consequência necessita de ser protegido apropriadamente.

O facto de os responsáveis dos organismos negligenciarem o factor segurança da informação, é referido por Straub & Welke (1998), como causa de potenciais incidentes de segurança nas organizações. Essa ameaça pode explorar vulnerabilidades de um activo ou conjunto de activos do qual pode resultar prejuízo no sistema e falhas de segurança da informação, este factor denomina-se risco, e poderá ser medido em termos da combinação da probabilidade de um evento ocorrer (ex. uma ameaça explorar vulnerabilidades) e as perdas ou prejuízos causados num activo ou grupo de activos, (ISO/IEC 13335-1, 2004).

Tendo por base a necessidade de gerir de forma optimizada todo o risco associado aos SI, surge o conceito de gestão de risco, Wright (2006) evidencia a necessidade desta gestão ser visível, com capacidade de identificar e encaminhar riscos para o necessário tratamento, controlando os riscos de segurança que podem afectar os sistemas de informação (SI), a um custo aceitável.

Outro conceito utilizado ao longo do trabalho, e associado ao risco de segurança, é o da vulnerabilidade ou nível de exposição que pode ser considerado como uma fraqueza de um activo ou conjunto de activos, que pode ser explorada por uma ou mais ameaças. Este factor ajudou a correlacionar o nível de cumprimento dos controlos de segurança com o nível de exposição ou vulnerabilidade respectivo priorizando desta forma as acções a tomar no âmbito da definição de um plano de segurança.

1.4.Sistema de Gestão da Segurança da Informação

Um ISMS pretende garantir como modelo, tal como refere ISO/IEC 27000:2009 (2009), os meios para implementar, operacionalizar, monitorizar e melhorar a protecção da informação e respectivos activos, de forma a alcançar os objectivos de negócio, com base numa avaliação e gestão do risco. Esses meios podem passar pela aplicação de controlos de garantia à protecção referida e de garantia do sucesso da implementação do ISMS. A ISO/IEC 27000:2009 (2009) define, entre outros, os seguintes princípios orientadores para o sucesso da implementação de um ISMS: Consciência da necessidade e atribuição de reconhecimento e responsabilidade à segurança da informação; Factor segurança assumido como elemento essencial nas redes e SI; Compromisso comum da gestão e respectivos *stakeholders*; Avaliação de risco com indicações de controlos adequados para atingir níveis aceitáveis de risco; Prevenção e detecção activa de incidentes de segurança da informação com avaliações contínuas e realização dos necessários ajustes.

A importância de um ISMS abrange diferentes vertentes, humana, física e tecnológica relacionada com a ameaça à informação dentro e fora da organização. O êxito de um ISMS garante à organização eficácia na protecção dos seus activos e processos, avaliação contínua e aplicação das boas práticas e controlos, com medição e aperfeiçoamento da sua eficácia, além de garantir a conformidade legal e regulamentar por parte da organização.

Esta norma foi precedida pela norma ISO 17799, definida pelo Instituto de Normas Britânico (BS7799), foi adoptado pela ISO/IEC tornando-se num código de boas práticas conjuntamente com as normas dentro da família ISO/IEC 27000. Esta norma encontra-se assente no ciclo PDCA, sendo este um dos princípios de funcionamento dos sistemas de gestão das normas ISO.

2. Revisão da Literatura

Toda a revisão bibliográfica planeada, assenta essencialmente em literatura referenciada na área dos SI, bem como na área da gestão da segurança dos sistemas da informação. A pesquisa de literatura foi realizada em diferentes áreas chave: área de regulamentação associada a segurança da informação, modelos e ferramentas, bem como casos de estudo que suportam estudos e modelos teóricos de gestão de segurança da informação.

Pretende-se adquirir conhecimento científico relevante nas áreas referidas, permitindo encontrar respostas para as questões e problemas enunciados. Desta forma, a revisão bibliográfica enquadra o estado da arte das áreas de investigação enunciadas.

Da revisão bibliográfica realizada, foram identificados vários autores e informação diversa dentro da área de investigação, onde se salienta Straub & Welke (1998) que já em 1998 assinalava a importância de um modelo de planeamento de segurança como forma de apoiar a tomada de decisão. Este conceito incidia desde logo na necessidade de conhecimento, definição e formalização do risco de segurança, bem como na utilização dos respectivos controlos para um planeamento de segurança, delegando responsabilidade na organização e nos seus recursos, optimizando-os alocando recursos em áreas previamente identificadas como deficitárias. Validando ainda no seu estudo que o problema da falta de segurança em algumas organizações podem e devem ser corrigidas internamente, existindo recursos, aptidão interna e *frameworks* para esse planeamento. Apesar de existirem excelentes consultores de segurança externos, que poderão ajudar nesse planeamento, é internamente que esse conhecimento deverá existir e que deverá ser aproveitado. Da metodologia apresentada pelo autor, salienta-

se o facto de existir alguma preocupação com o envolvimento da organização em todo o processo, bem como planos internos de consciencialização dos problemas associados à segurança, sendo que esta metodologia assenta em três passos principais: (1) Existência de um plano de segurança (2) Consciencialização para o risco de segurança com planos de formação internos (3) Uma matriz de análise de contramedidas, conforme Figura 1-1.

Em 2002 através do Instituto de Normas Britânico é definido o *standard* BS 7799-2:2002 que dará lugar, em 2005, à norma ISO/IEC 27001:2005 (2005) referenciada ao longo do estudo de caso na sequência dos requisitos para a implementação do SGSI. Associado a este *standard* surgem os respectivos controlos ISO/IEC 27002:2005, utilizados como guia de implementação a utilizar em todo o processo.

Na sequência do aparecimento de controlos e guias de monitorização dos processos de implementação, encontramos na literatura o estudo de Wright (2006) promovido pela *Siemens Insight Consulting.* O autor verifica no seu estudo de caso a necessidade da implementação efectiva de um ISMS, bem como da necessidade de identificar e medir através dos controlos e *standards ISO/IEC,* referidos anteriormente, por forma a alertar a organização para possíveis incidentes de segurança, demonstrar a eficácia da implementação, bem como consciencializar a gestão para o problema, em conformidade com o referido por Straub & Welke (1998). Refere que, deve ser definida uma estratégia clara de quais as medidas a usar, para efectivamente medir a eficácia da segurança e do respectivo ISMS. Neste sentido o autor classifica os controlos/medidas em várias categorias, com identificação dos *itens* necessários e tangíveis de serem medidos e auditados.

Em 2007, e ainda no seguimento de processos de certificação e de implementação de SGSI, Santos (2007) e Coelho (2007), nos seus diferentes trabalhos de investigação, identificam alguns factores chave a considerar associados aos seus casos de estudo. Santos (2007), num estudo de caso centrado na área hospitalar, valida que qualquer política de segurança terá de obedecer a um processo de gestão do risco, e que é premente o envolvimento da organização nesse processo, criando uma metodologia própria associada ao sector, no âmbito do cálculo do risco para o caso específico. Este envolvimento global cria uma vertente formadora e sensibilizadora, educando para a problemática da segurança. De referir, que este autor assemelha-se de alguma forma com o referido anteriormente por Straub & Welke (1998) e Wright (2006) em termos de metodologia e abordagem de implementação. Por outro lado Coelho (2007), ressalva o facto de apesar da importância da definição de um modelo de gestão para a segurança da informação, e do facto de esse sistema permitir uma redução substancial do risco de uma organização, é importante assumir o factor custo, associado à implementação e inserção de novas actividades e responsabilidades dentro da organização (no estudo de caso um aumento de 20%), além de um incremento do investimento respectivo em controlos de segurança. Assume ainda, que terá de existir um pesado envolvimento dos funcionários, no processo de implementação e definição do âmbito do sistema de toda a organização, e em especial da equipa de implementação (no caso específico cerca de 53 dias úteis contínuos, apenas para projectar e implementar um processo de gestão do risco). Aliado ao envolvimento da organização, surge também a questão associada à especificidade da organização e respectivas características, tendo Oliver (2007) comparado no seu estudo 3 diferentes organizações. O autor analisa a implementação de *standards* e *frameworks* (*ISO 15489-1:2001*

Information and documentation -- Records management), verificando que as estratégias de implementação devem ser adaptadas as organizações, nomeadamente o seu contexto cultural, social, quadro normativo e legislativo. Constatando que a compreensão destes factores num quadro de gestão da implementação, favorece o sucesso da implementação de normas e *standards* internacionais.

Sendo cada vez mais sensível e actual a questão da segurança da informação, surge em 2008 o relatório Office (2008), da responsabilidade do *Cabinet Office UK*, gabinete de assessoria do primeiro ministro do Reino Unido, que identifica e estabelece normas na área da gestão do risco e segurança da informação. O relatório, em alinhamento com os anteriores autores, promove a necessidade de estabelecer *standards* coesos dentro das organizações, bem como controlos de gestão e controlo das infra-estruturas tecnológicas. Identifica ainda, a aplicação de métodos de gestão da informação, de forma a promover a compreensão da gestão do risco, alinhados sempre com a gestão do negócio e a própria gestão de topo. Este gabinete, promove junto dos seus organismos a necessidade de ajustar mecanismos de segurança à realidade actual, bem como manter o foco contínuo na questão da segurança da informação e processos de gestão do risco, nomeadamente, fortalecer os mecanismos de responsabilização dos departamentos dentro da organização, bem como reforçar a sua análise de desempenho. O relatório descreve ainda o *standard* ISO/IEC 27001:2005 (2005) como metodologia adoptada, centralizando a sua monitorização contínua de forma a assegurar conformidades e retirar conclusões e ajustamentos dos erros verificados. Promove também, a necessidade de processos de reciclagem e formação descentralizada, para promoção das boas práticas em termos de manipulação de dados e segurança da informação.

De acordo com a necessidade de avaliar as organizações e os seus factores de resistência, associados aos seus processos de formulação e implementação de ISMS, Lapke & Dhillon (2008) referem no seu artigo publicado em 2008, que existe uma clara evidência de resistência à implementação de sistemas de gestão e politicas de segurança dentro da organização, provocadas por diversas forças de resistência internas, sendo necessário criar as necessárias relações entre elas para diminuir o impacto do estabelecimento destes procedimentos nas organizações. O factor relações de poder dentro da organização, por vezes complexo, tem um claro impacto sobre o processo da gestão da segurança, nomeadamente, a percepção do impacto dessa aplicação na produtividade, o poder de determinados grupos especialistas na área, e a sua influência na formulação e implementação dos processos.

Nesta linha de actuação Smith (2010), efectua no seu estudo uma análise detalhada ao processo de implementação e certificação de ISMS em organismos públicos, interpretando através de modelos específicos para o efeito, toda a componente associada à resistência na adopção de *standards*, especificidades culturais e toda a envolvente associada ao organismo. O autor realça a importância da utilização de uma estratégia de implementação, baseada em estruturas/organizações mais pequenas, por forma a garantir um maior controlo e motivação para o tema, ajudando desta forma a condução do processo de certificação. Identifica ainda alguns factores como preconceitos culturais ou métodos/normas de grupo dentro dos organismos, que incutem resistência à implementação, além das já mencionadas falta de recursos, nível de especialização e compromisso da gestão de topo. Outra das questões verificadas, foi a falta de definição conjunta de uma política e gestão de segurança comum

entre os vários organismos, tendo em conta que existe autonomia dos vários organismos para definirem os seus processos individualmente.

Ainda dentro da literatura referenciada, no que concerne à implementação de ISMS, surgem em 2009 alguns trabalhos de investigação que avaliam a implementação em pequenas e médias empresas (PME), e que estudam de forma pertinente a adaptação dos modelos tradicionais a esta realidade empresarial. Neste sentido, torna-se importante verificar através de bibliografia existente, como estes *standards* e modelos se adaptam a diferentes realidades e a diferentes organizações. Siponen & Willison (2009), analisam os problemas e soluções associados a diferentes organizações, na sequência da implementação do respectivo ISMS, e referem que apesar de ser aceite que a implementação de um ISMS desempenha um papel fundamental, na segurança da informação das organizações, cada caso é um caso. É importante salientar que os *standards* são muito abrangentes, ignorando muitas das vezes as diferenças e especificidades das organizações, os seus requisitos e orientações específicas de segurança, em linha com o referido por Smith (2010) e Oliver (2007). Tal facto, pode levar a que o processo se torne mais susceptível e falível durante a sua implementação. Os autores, à imagem do que refere Straub & Welke (1998), reforçam a teoria de que uma auto-avaliação é importante em todo este processo para conhecer as especificidades da organização. Outros dos autores que descrevem esta problemática são Valdevit, et al. (2009), que se centram em definir um guia de soluções de implementação para o caso especifico de PME´s, verificando que se trata de casos específicos e que os modelos terão de se ajustar a estas realidades. Este guia, dá a possibilidade aos utilizadores de se concentrarem nos elementos fundamentais de uma implementação ISMS, levando a um aumento significativo dos níveis de eficiência na sua aplicação. Identifica também,

à semelhança de outros autores citados anteriormente, a importância de um âmbito e objectivos bem definidos, bem como a realização de auditorias internas para avaliar metas e necessidades em relação ao estado de implementação de um ISMS.

Em 2011, Gillies (2011) apresenta um estudo motivado pelo avanço das tecnologias, e da importância cada vez mais significativa da protecção da informação, associado também neste caso a PME´s. O autor menciona que a implementação dos padrões ISO/IEC 27000, apresentam fracos níveis de adopção, apesar da necessidade premente identificada de recorrer a *standards* e metodologias de gestão, identificando como causa principal o facto de estes padrões serem excessivamente complexos e onerosos para muitas organizações, por exemplo, de pequeno porte. Desta forma, o autor tenta desenvolver uma abordagem mais simplificada, que promova a redução de algumas barreiras da implementação, facilitando o seu acesso a este tipo de organizações. Este estudo reforça estudos anteriores, que identificam a necessidade de se ajustar as metodologias às organizações, e suas especificidades.

Durante 2011 surgem alguns relatórios que definem o estado actual deste tipo de áreas de investigação, como é o caso do relatório ITSMF (2011), que avalia os níveis de Maturidade da Governação e Gestão de TI em Portugal, identificando a grande importância que as empresas portuguesas colocam na aposta em ISO/IEC 27000, a par de *frameworks* como ITIL (Information Technology Infrastructure Library), sendo consideradas em Portugal uma das fontes de orientação e referência em *information security.* O relatório revela, que em determinadas empresas ainda identificam a função de responsabilidade da gestão da segurança da informação como acessória, e realizada em *part-time,* existindo também organizações com

definição efectiva de responsabilidades assegurando essa função de gestão da segurança da informação. Analisa também, o factor definição formal das Políticas e Normas de Segurança da Informação, existindo neste caso um *deficit* de formalização destes documentos, ou nalguns casos estes documentos encontram-se desactualizados e/ou omissos em áreas chave.

Recentemente, surgiu também um relatório da ENISA, (ENISA, 2012), que identifica e alerta para a importância da avaliação do risco, como uma das componentes chave e central de qualquer sistema de informação de gestão de segurança padrão, sendo apontada a identificação e avaliação de activos como factor decisivo, uma vez que apoia a fase de determinação do sistema de referência, em que a avaliação do risco será baseada. Identifica a importância da recolha e levantamento da informação, para avaliação em todo o ciclo de implementação, a importância da definição de procedimentos de gestão de risco, de metodologias e medidas adequadas tecnologicamente, planos de identificação de responsabilidades, bem como promoção de testes aos respectivos planos. Todas estas indicações, encontram-se de acordo não só com o modelo conceptual definido, que teve por base a *framework* ENISA, Figura 1-2 *Framework* ISMS da ENISA, e plano de segurança (Straub & Welke, 1998), bem como toda a revisão bibliográfica de referência analisada.

De referir por último, que a recente Resolução do Conselho de Ministros (Presidência do Conselho de Ministro, 2012), está de acordo com a *framework* e relatório ENISA, aplicando as orientações europeias em matéria de interoperabilidade ENISA, onde são definidas um conjunto de directrizes que os SI da Administração Pública devem obrigatoriamente seguir. Definem ainda a implementação de uma estratégia nacional de segurança da informação, entre

outras a implementação de ferramentas e metodologias de catalogação TIC, e a definição de normas e directrizes de segurança sectoriais, além da responsabilidade de identificar os responsáveis pela implementação da segurança da informação no país, bem como responsáveis por estabelecer, controlar, medir e gerir o risco e auditar a segurança da informação.

Em conclusão, verificamos com as hipóteses levantadas que toda a bibliografia faz referência à importância de um modelo de planeamento de segurança, que permita gestão e avaliação do risco associado à segurança da informação, ou seja, um SGSI capaz de consciencializar a organização com as boas práticas e ferramentas e os seus recursos internos, garantindo uma melhor avaliação e optimização de recursos e procedimentos, em termos de eficácia no planeamento de segurança.

A revisão bibliográfica, identifica também a importância da informação e a sua segurança, classificadas como vitais para a organização e respectivo negócio, desde que alinhados com a sua política de segurança definida de uma forma clara e objectiva. Os factores de insucesso estão identificados e classificados, bem como o contributo da utilização das boas práticas na área da segurança dos SI, quer em processos de avaliação prévia, proposição a ser testada no estudo de caso apresentado, quer na prossecução da implementação dos respectivos processos de ISMS.

3. Metodologia

De acordo com a questão de investigação (Qual o contributo de um processo de auto-avaliação interna prévio ISO27002, na implementação de um Sistema de Gestão da Segurança da Informação?), que procura explorar qual ou quais os contributos da *framework* apresentada, podemos justificar a utilização de uma estratégia de investigação com base na condução de um estudo de caso exploratório, com o objectivo de formular hipóteses e proposições relevantes para investigação futura (Yin, 1994) .

Por outro lado, a adopção de um estudo de caso, como refere Caldeira (2000), permite uma compreensão aprofundada do objecto de investigação, não pretendendo ser uma amostra estatisticamente válida da população, onde um ou dois casos podem ser suficientes para conduzir uma investigação e chegar a conclusões válidas. Desta forma procura-se uma generalização analítica, como também defende Yin (1994), referindo que estudos de caso únicos também são generalizáveis para proposições teóricas (generalização analítica), e não para populações ou universos (generalização estatística).

Existem várias aproximações para a definição de objectivos de um estudo de caso: para Yin (1994), o objectivo do estudo de caso é explorar, descrever ou explicar um fenómeno ou facto observado, e segundo Guba & Lincoln (1998) o objectivo é relatar os factos como sucederam, descrever situações ou factos, proporcionar conhecimento acerca do fenómeno estudado e comprovar ou contrastar efeitos e relações presentes no caso. Sendo o objectivo geral de um estudo de caso, sistematizado pelos autores anteriormente referidos Yin (1994) e Guba & Lincoln (1998), “explorar, descrever, explicar, relatar e/ou descrever factos”, é importante

referir que a apresentação do caso específico deverá garantir conteúdo de investigação para testar, comprovar, confirmar ou responder a determinadas questões ou hipóteses assumidas, conforme refere Guba & Lincoln (1998).

No intuito de se obter maior conhecimento sobre o tema, em torno de um problema ou questão de investigação, em que são limitados os estudos anteriores sobre a questão formulada, é usado o método exploratório, levantando hipóteses de entendimento de algumas realidades verificadas, nomeadamente verificadas no estudo de caso apresentado. De referir que o conhecimento existente sobre o tema encontra-se focado essencialmente no processo conducente à implementação de um plano de segurança da informação, onde existem para o efeito alguns casos de estudo com a demonstração dos modelos instituídos e problemas verificados. Demonstrações e casos de estudo referidas ao longo da revisão bibliográfica.

Neste estudo de caso é seguida uma abordagem essencialmente qualitativa, aplicada ao problema identificado. É realizada uma recolha, observação, selecção, análise e interpretação dos dados, e onde se inclui também algum conhecimento empírico através da observação de determinadas situações, levando a gerar conceitos, ideias e padrões encontrados nos dados pelo investigador, participante, assumindo neste caso uma importância extrema o facto de a equipa multidisciplinar de trabalho no organismo, ser constituída por varias valências transversais à organização e aos SITI, garantindo não só valor académico como mais-valia na avaliação dos dados, dado que os dados foram analisados anteriormente por diferentes avaliadores (triangulação). Trata-se da exploração de um fenómeno limitado no tempo, onde é realizado um estudo indutivo e descritivo, mas também intensivo e detalhado de uma entidade

bem definida, única e específica. As unidades e variáveis de análise são as seguintes: organização, dimensões e controlos ISO/IEC 27002; nível de cumprimento, vulnerabilidade e nível de exposição.

A fonte principal de recolha de dados é a base de dados (Microsoft Access) pertencente ao organismo alvo de análise (SGMOPTC), que contem o histórico realizado das unidades e variáveis de seguranças avaliadas (controlos). Foram realizados procedimentos de recolha dos documentos num único momento (final de 2011) dos registos em tabelas de base de dados, para tratamento gráfico, analise e avaliação conforme exposição realizada no capítulo 4.3 – Estudo de caso – descrição, e respectiva análise de resultados descrita no capítulo 5 – Análise de resultados. Desta avaliação resultou um relatório dos dados observados, submetido para aprovação ao dirigente máximo do serviço (Secretário-Geral do MOPTC).

Este conhecimento permitiu, ao longo da investigação, a comparação do estudo de caso com outros autores e casos de estudo semelhantes, ou métodos de análise implementados, resultantes da revisão bibliográfica realizada, sendo possível correlacionar essas ideias e formular as necessárias relações entre elas.

O método é adequado na resposta à questão de investigação anteriormente apresentada.

4. Estudo de caso

4.1.Enquadramento

A Secretaria - Geral do Ministério das Obras Publicas Transportes e Comunicações (SGMOPTC), organismo do sector público – Administração Central do Estado, tem como principal função apoiar os gabinetes dos membros do Governo, bem como todos os órgãos e serviços do Ministério nos domínios administrativo e técnico, além da responsabilidade de guarda e gestão do património imobiliário e documental do Ministério.

De acordo com as suas unidades orgânicas, a SGMOPTC presta diferentes serviços conforme anexo E, Tabela 9-1 Unidades orgânicas e serviços prestados. De acordo com as suas várias atribuições a SGMOPTC tem atribuída, dentro da função de Gestão de Tecnologias de Informação e Comunicações, a competência para definir e implementar as políticas relacionadas com as tecnologias de informação e comunicações do MOPTC, garantindo a coordenação, execução e avaliação das iniciativas de informatização e actualização tecnológica dos respectivos serviços e organismos, assegurando uma gestão eficaz dos recursos disponíveis, conforme (Decreto Regulamentar n.º 60-A/2007, s.d.). Assim a DSTIC presta serviços TIC diferenciados a diversos clientes conforme anexo F, Tabela 9-2 Listagem de clientes SGMOPTC.

Tendo em conta o quadro de avaliação e responsabilização de 2011 (QUAR) da SGMOPTC, (SGMOPTC, 2012), este organismo no âmbito da sua missão estabelece três objectivos estratégicos transversais a toda a organização: Melhorar a qualidade do serviço prestado aos clientes da SGMOPTC; Contribuir para a racionalização da despesa pública, optimizando os

recursos financeiros disponíveis e melhorar o modelo organizacional, com vista a uma gestão por resultados.

Considerando que em 2010 a DSTIC desenvolveu uma Arquitectura de SI, em que uma das entidades (grande objecto de gestão) da SGMOPTC é a segurança, conforme (SGMOPTC Arquitectura, 2011), foi decidido que tendo em conta os objectivos estratégicos atrás referidos, um dos objectivos operacionais no âmbito das TIC seria: melhorar a qualidade e segurança das tecnologias de informação e comunicações disponibilizadas, realizando uma auto‐avaliação ao sistema de segurança da informação pela Norma ISO/IEC 27002:2005.

Com base nos objectivos estratégicos traçados pela gestão de topo, e consequentemente atribuído o objectivo operacional à DSTIC, iniciou-se o procedimento para definição do âmbito do sistema de auto-avaliação de segurança da informação da SGMOPTC, tendo como base de trabalho o documento de política de segurança e privacidade do organismo, (SGMOPTC Arquitectura, 2008). Com o objectivo claro de melhorar a qualidade e segurança da informação prestada, através da aplicação de uma auto-avaliação interna, cumprindo a norma (ISO/IEC 27002:2005, 2005), a equipa de trabalho começou por reunir toda a informação necessária que caracterizasse o conhecimento da organização e respectivos objectivos de negócio, garantindo desta forma um alinhamento eficaz entre organização, negócio e os seus SI. Definida a utilização das boas práticas, iniciou-se a construção de uma *framework* que garantisse a concretização dos objectivos estratégicos propostos, bem como o estabelecimento de uma estrutura base de um SGSI para a SGMOPTC.

O estudo apresentado, foi realizado por uma equipa multidisciplinar (2 técnicos superiores da Divisão de Sistemas de Informação e 2 técnicos superiores da Divisão de Qualidade) afecta à SGMOPTC, onde participei como coordenador técnico do estudo realizado. Para o efeito, foram decisivas as competências técnicas e académicas adquiridas ao longo da minha carreira profissional, salientando o facto de ter participado como responsável do documento de política de segurança e privacidade da SGMOPTC, em diversas auditorias de segurança da informação, comissões de acompanhamento e definição estratégica TIC, além da consequente formação complementar especializada em comunicações, redes e segurança e formação académica em engenharia electrotécnica, que me garantiram uma visão mais abrangente da organização, bem como um conhecimento mais especializado dos temas abordados neste trabalho de investigação.

4.2.Auto-Avaliação com recurso a controlos ISO 27002:2005

Existem diversas formas de identificar ou estabelecer os requisitos de segurança mais adequados à organização. A (ISO/IEC 27002:2005, 2005) identifica pelo menos três: 1. avaliando a organização, a sua estratégia e objectivos de negócio identificando vulnerabilidades e probabilidades de ameaça aos seus activos estimando este impacto; 2. Através do estabelecimento e cumprimento legal, estatutário, ou contratual a que se encontra vinculado dentro do seu contexto sociocultural; 3. Outra forma é através dos princípios normativos internos desenvolvidos para o manuseamento e operação da informação que a organização estabelece para o suporte ás suas operações. No estudo de caso apresentado foram estabelecidos os requisitos através da avaliação da organização, identificando vulnerabilidades

e probabilidades de ameaça aos seus activos tendo em conta os pontos de falha, dos níveis de cumprimento, níveis de exposição/vulnerabilidades e respectivas áreas de responsabilidade.

Os controlos definidos no *standard* incluem diferentes áreas de intervenção, incluindo controlos administrativos, técnicos e legais. Caracterizam-se, conforme referido no *standard* em 11 diferentes cláusulas de controlo de segurança, apresentando diferentes categorias (cerca de 40) dentro dessas cláusulas principais. É dentro das categorias referidas que se encontram os diferentes controlos (cerca de 130), objecto de análise ao longo do estudo de caso. As cláusulas de controlo de segurança encontram-se em anexo G, Tabela 9-3 Clausulas de controlo de segurança.

Apesar da definição efectiva dos 133 controlos, a organização pode no entanto estabelecer e adoptar controlos próprios, que traduzam de forma mais eficaz a sua realidade, documentando no SGSI a sua aplicabilidade. Neste caso, houve cerca de seis controlos definidos no *standard* não utilizados, devidamente fundamentados.

A monitorização e gestão dos controlos estabelecidos, são essenciais para a correcta definição da estrutura de responsabilidade da informação. Estes controlos e objectivos, podem ser transversais a diferentes áreas ou unidades organizacionais, partilhados ou indexados a diferentes estruturas/áreas existentes. Toda a organização foi envolvida a participar e a manter o sistema de gestão ao longo do tempo, criando desta forma dependência organizacional, quer entre departamentos quer entre responsabilidades das áreas departamentais e responsabilidades associadas à segurança da informação.

4.3.Estudo de caso – descrição

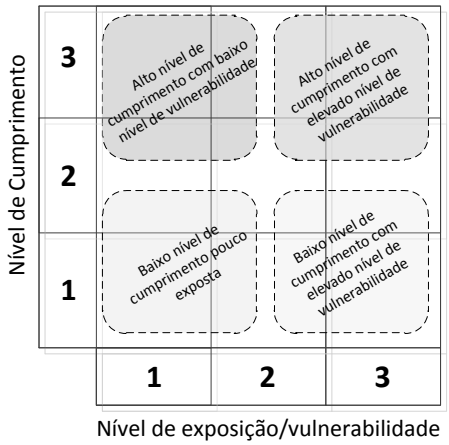
Relativamente ao contexto empírico da investigação, são apresentados de seguida os eventos sumários que podem ser observados no estudo de caso e que sustentam a investigação realizada. Este estudo de caso e o respectivo mapa de controlo, procura estabelecer métricas e apontar propostas de implementação, no sentido de melhorar e aperfeiçoar os pressupostos de implementação da segurança da informação, com base na norma (ISO/IEC 27002:2005, 2005).

Depois de efectuada a recolha dos dados, foram criadas diferentes dimensões de análise dos controlos estabelecidos, com identificação dos seus pontos de falha, níveis de cumprimento, níveis de exposição/vulnerabilidades, e respectivas áreas de responsabilidade do controlo dentro da organização. Como se pode verificar pela figura seguinte, o mapa de controlos é construído pela equipa multidisciplinar de trabalho, a partir da classificação dos diferentes 133 controlos (ISO/IEC 27002:2005, 2005) nas várias dimensões, da seguinte forma: Em relação à classificação de cumprimento, atribuição de ponderação 3 no caso de a SGMOPTC cumprir na íntegra o estabelecido pelo objectivo de controlo; atribuição de ponderação 2 no caso de a SGMOPTC cumprir parcialmente o controlo ou se encontrar em curso determinadas acções para o seu cumprimento; atribuição de ponderação 1 no caso de o organismo não cumprir o estabelecido no controlo; atribuição de ponderação 0 (zero) caso o controlo não se aplique ao caso específico da SGMOPTC.

Em relação ao nível de classificação do nível de exposição/vulnerabilidade, foram também analisados os 133 controlos, com atribuição de ponderação 3 no caso de o controlo em causa, ou o seu não cumprimento, potenciar um nível de exposição elevado da segurança da

informação do organismo, tornando-se vulnerável a potenciais ameaças de segurança internas ou externas; atribuição de ponderação 2 no caso de o controlo permitir um factor de exposição parcial em que apenas coloque vulneráveis determinados sectores onde existem em curso determinadas acções para a sua resolução; atribuição de ponderação 1 no caso de o controlo apresentar baixos níveis de exposição ou vulnerabilidade a ameaças da segurança da informação da organização; atribuição de ponderação 0 (zero) caso o controlo não se aplique ao caso específico da SGMOPTC.

As duas dimensões, foram analisadas isoladamente e correlacionadas de seguida, permitindo obter uma matriz com a intersecção das duas análises. A informação resultante é crucial na análise da percepção do risco de segurança, tendo em conta que consegue estabelecer quais as áreas mais críticas em termos de cumprimento, face ao seu nível de exposição/vulnerabilidade. Como tal, é possível caracterizar áreas mais abrangentes, cláusulas de segurança específicas, ou isoladamente os controlos respectivos, permitindo canalizar recursos para áreas mais críticas.



Fonte: Estudo de caso SGMOPTC – Matriz de dimensões de análise

Figura 4-1 Matriz de dimensões de análise

Numa segunda fase, foram analisados todos os objectivos/metas respectivos, e atribuído um departamento responsável pelo seu cumprimento/incumprimento, dentro das unidades orgânicas existentes no organismo, conforme Tabela 9-1 Unidades orgânicas e serviços prestados. Posteriormente, foi correlacionada esta informação com os níveis de cumprimento dos controlos, permitindo criar uma matriz, onde para cada um dos controlos existe qual a entidade responsável pelo seu cumprimento, e qual o objectivo/meta que deve atingir.

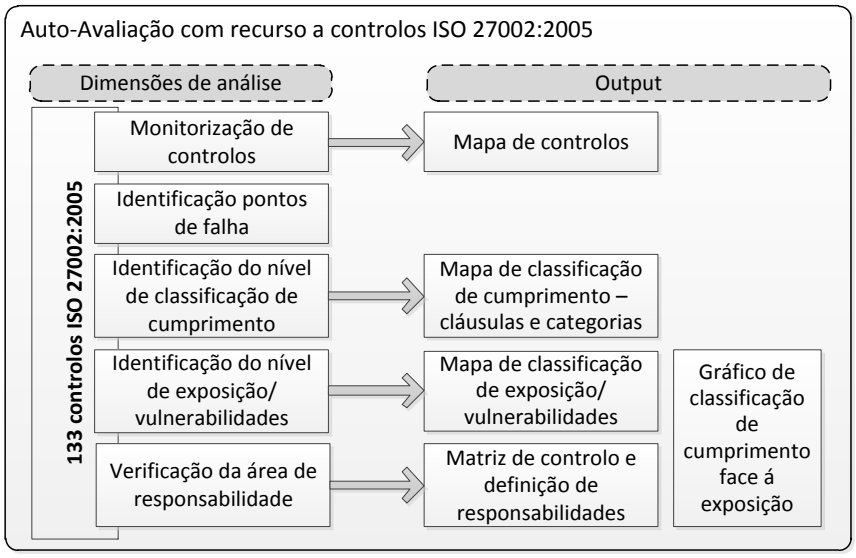
Em termos de análise sumária dos resultados obtidos, através da análise do mapa de controlos, verificamos que o nível de classificação médio de cumprimento dos controlos é de 2,16, ou seja cerca de 45.6% de cumprimento. Com pior desempenho, em termos de cumprimento médio, identifica-se a categoria A.6 (Organização da segurança da informação) e A.8 (Segurança de recursos humanos), áreas onde se devem concentrar recursos para mitigar estas falhas.

Em relação ao nível médio de exposição/vulnerabilidades é de 1,65, para a totalidade dos níveis de cumprimento, em relação aos níveis de exposição com classificação de cumprimento 1-2 é de 1,67; nível 3 aumenta ligeiramente para os 1,67; nível 1 diminui para 1,56. Verifica-se que as categorias de controlo com maior nível médio de exposição/vulnerabilidade são a categoria A.6, A.8 e A.9 (Segurança física e ambiental), constituídas essencialmente por controlos em relação a organização e entidades externas ao organismo, definição de políticas de segurança dos colaboradores, e controlos que verificam a exequibilidade do estabelecimento de plataformas de controlo da segurança física, e ambiental dos sistemas.

Em casos específicos existia desconhecimento, falta de consciencialização, de determinados controlos/ necessidades em termos de segurança dos sistemas e informação, e necessidade de

envolvimento e optimização dos recursos da organização. Alguns controlos tiveram por parte dos sectores responsáveis, um tratamento imediato quando alertados. Por exemplo, articulação da gestão do edifício (DRP) com necessidades de gestão do centro de dados (DSTIC).

Esta ferramenta, procura ainda fornecer os necessários *outputs* de análise, não só para a equipa responsável pela gestão do plano de segurança da informação do organismo, mas também informação estratégica de gestão de recursos para a gestão de topo, garantindo conhecimento, alinhamento com o negócio e enquadramento das boas práticas na organização. Esta auto-avaliação, pretende suportar a tomada de decisão, além de contribuir para o aumento da eficácia na implementação do SGSI. Factos que enquadram a resposta às questões de investigação e consequente enquadramento teórico. A Figura 4-2 demonstra de forma sumária os pressupostos de análise bem como a informação resultante após classificação das dimensões por parte da equipa de trabalho. Os *outputs* resultantes encontram-se em anexo A,B,C e D.



Fonte: Estudo de caso SGMOPTC

Figura 4-2 *Framework* de Auto-Avaliação

5. Análise de resultados

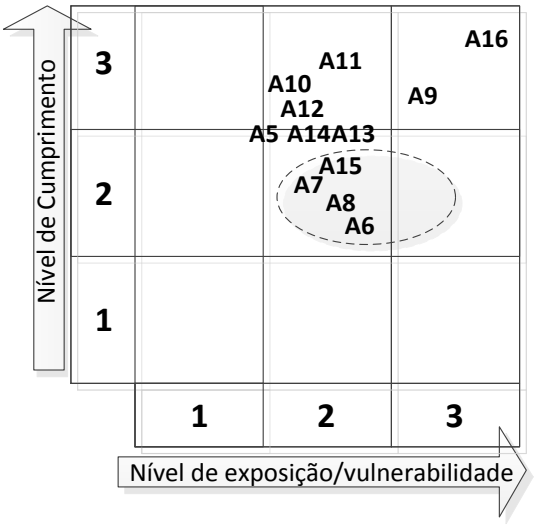
De acordo com a descrição do estudo de caso, apresentada no capítulo anterior, surgem alguns factores que merecem ser analisados tendo em conta os resultados apresentados.

Dos *outputs* extraídos da *framework,* salienta-se o facto de ser possível identificar de forma clara, as áreas onde se deve aplicar esforço bem como uma maior consciência de toda a organização para o ISMS. Como menciona Straub & Welke (1998), o reconhecimento e consciência do problema, existindo percepção do risco nas diferentes áreas de intervenção, torna possível estabelecer planos de decisão mais abrangentes à organização. O factor ambiente organizacional, e as características individuais das áreas envolvidas (Straub & Welke, 1998) são um factor determinante para o reconhecimento do problema, tendo em conta que é possível depois do processo da auto-avaliação, organizar tarefas e procedimentos internos, controlar responsabilidades e metas no mesmo plano de gestão de segurança. Esse ajuste de dependências é verificado através dos mapas extraídos, por exemplo, entre DSTIC, DRP e DRH.

O caso específico da DSTIC, que participa directa ou indirectamente em 131 dos 134 controlos analisados, foi identificado e tomado em consideração nas revisões do documento de políticas de segurança (SGMOPTC Arquitectura, 2008), comprometendo a organização no reforço das equipas de segurança alocadas à DSTIC, aquando da próxima afectação de pessoal. A definição de políticas de segurança, definido como primeiro passo na *framework* ENISA (2012) para o estabelecimento de um ISMS, faz sentido se avaliado previamente o seu enquadramento na organização, ou seja, é importante avaliar e enquadrar a organização previamente em termos de conhecimento da segurança da informação, de uma forma cíclica e realimentada com os

necessários ajustamentos, como sugere Straub & Welke (1998), garantindo desta forma políticas de segurança mais consistentes, com monitorização continua e eficaz, bem como planos de risco de segurança mais aproximados da realidade da organização e do ISMS.

Por outro lado, podemos identificar e avaliar dentro das 11 cláusulas de controlo de segurança, quais as áreas mais críticas. Do cruzamento desta informação, avaliada nas duas dimensões, é possível verificar que existem cláusulas ou áreas de segurança com baixos níveis de cumprimento para níveis elevados de vulnerabilidade/exposição, alertando para o elevado risco em termos de segurança para a organização. Na prática, verificou-se que os piores níveis de cumprimento se encontravam nas cláusulas de controlo de segurança A6; A7; A8; A15, sendo que os piores níveis de vulnerabilidade/exposição se encontravam nas clausulas A6; A8 e A9, levando a concluir, que é nas cláusulas A6 e A8 que devemos incidir o nosso esforço e recursos, no sentido de colmatar as falhas existentes, facto que se pode constatar na figura seguinte.



Fonte: Estudo de caso SGMOPTC – Matriz de representação das cláusulas face ao seu nível de cumprimento e exposição

Figura 5-1 Matriz de nível de cumprimento e nível de exposição das cláusulas de controlo de segurança

Se analisarmos mais em concreto a clausula A6 – Organização da segurança da informação, onde a classificação média atribuída foi de 1,55 e 1,82 (nível de cumprimento e nível de vulnerabilidade/exposição respectivamente), verificamos que poderão existir problemas associados à segurança da informação em duas categorias de controlos, A6.1 – Organização interna e A6.2 – Partes externas, categorias que integram a cláusula A6. Da informação retirada dos mapas de classificação de cumprimento, em anexo B, a cláusula A6.1 apresenta uma classificação média de 1,5 e 1,38 e a cláusula A6.2 apresenta uma classificação média de 1.67 e 3 para os níveis de cumprimento e nível de vulnerabilidade/exposição respectivamente. Como tal, conseguimos rapidamente identificar o motivo de não cumprimento, consultando o mapa de controlos e verificar que os problemas essenciais se encontram nos controlos A6.1.2 - Coordenação da segurança da informação; A6.1.5 - Acordos de confidencialidade e A6.2.1 - Identificação dos riscos relacionados com partes externas. Da análise realizada aos objectivos destes três controlos, que revelam incumprimento, constatamos que não existe no organismo o levantamento dos riscos para a informação, e recursos das entidades externas ao organismo, não existem acordos de confidencialidade estabelecidos em relação a protecção da informação, e não existem actividades de coordenação formalmente estabelecidas no âmbito da segurança da informação. Serão estas as medidas a estabelecer e a afectar aos departamentos (no caso específico dentro do organismo de acordo com a matriz de controlo de responsabilidades (A6.1.2: Gestão de topo e DSTIC; A6.1.5: DSTIC; A6.2.1: DSTIC).

No estudo de caso apresentado constatou-se que alguns dos controlos (cerca de seis) não seriam considerados, como é o caso do controlo A10.9 ou A12.3 que identificam objectivos de controlo para transacções de comércio electrónico ou serviços e conformidades criptográficas,

não existindo aplicabilidade prática na SGMOPTC, ou seja, o ajuste e selecção de controlos, (ENISA, 2012), é importante, já que nem todos os controlos ISO/IEC 27002:2005 (2005) se aplicam à mesma organização.

Uma das mais-valias desta *framework* é sem dúvida a possibilidade de percepção do risco de segurança da organização, com o auxílio das ferramentas (mapas, gráficos, tabelas e matrizes) extraídas da auto-avaliação, permitindo optimizar planos de acção de decisão e contramedidas em termos de implementação de segurança.

Ainda neste âmbito, de referir que a equipa responsável pelo processo de avaliação é ainda responsável por rever anualmente a política de segurança do organismo (SGMOPTC Arquitectura, 2008), tendo em conta que se tratam de processos correlacionados como apresentado no modelo conceptual. Ou seja, todo o processo de avaliação requer constante monitorização, com processos cíclicos de revisão do mapa de controlos, e consequentemente revisão dos documentos de política de segurança do organismo, na medida em que são aplicadas medidas de resolução e mitigação do risco de segurança, através da avaliação do cumprimento dos controlos, que terão de ser analisados em termos de eficácia, sempre alinhados com o negócio e consequentemente com a especificidade da organização.

6. Conclusões e considerações finais

Da investigação e resultados obtidos com o estudo de caso, e todo o conhecimento científico retirado da literatura analisada, é possível extrair algumas conclusões, bem como tentar responder de forma objectiva à questão de investigação formulada.

O estudo parece indicar que a utilização de um processo de avaliação prévia na implementação de um SGSI, contribui não apenas como forma de auditar e preparar a organização, optimizando planos e processos para uma implementação mais eficaz, mas também na antecipação do risco como garante do aumento da consciência interna para o problema da segurança. Desta forma, existe o garante de opções gestionárias consistentes, aumentando o nível de reconhecimento e responsabilização do problema, transversal a toda a organização, permitindo adequar o modelo a implementar à realidade do organismo.

Tendo em conta os inúmeros autores e modelos, que defendem a necessidade de adaptar as ferramentas às organizações e especificidades, e de acordo com o observado da não aplicação e adaptação de controlos no estudo de caso analisado, podemos referir que pode fazer sentido optar por uma auto-avaliação prévia da organização aquando da implementação de um SGSI, na medida em que contribui para optimizar e adaptar modelos à realidade verificada, quer em termos da segurança da informação quer à forma de implementação na respectiva organização. De referir, que quer a literatura quer o estudo de caso e *framework*, aponta para a necessidade de aposta no envolvimento da organização em todo o SGSI como forma de garantir o sucesso e eficácia dos planos de gestão da segurança da informação nos organismos.

7. Contributo e sugestões de trabalho futuro

Do estudo realizado, poderá ser retirada mais-valia académica das conclusões e resultados associados ao estudo de caso. Podemos assinalar o seguinte contributo resultante do trabalho de investigação realizado:

A investigação e estudo de caso, demonstram a relevância do enquadramento e alinhamento necessário com a organização do modelo conceptual proposto, em particular no sucesso de implementações ISMS. Confirmando desta forma, o modelo estabelecido e o contributo de uma avaliação prévia para a eficácia de um ISMS.

Tendo em conta que a literatura analisada, foca essencialmente a implementação de ISMS e *frameworks* dentro do ciclo de implementação PDCA, o modelo e *framework* apresentado pode ser também usada para análise de performance da organização fora do ciclo de implementação, possibilitando avaliar e ajustar todo o processo de implementação antecipadamente.

O estudo realizado complementa *frameworks* existentes analisadas e investigadas por diversos autores, tendo em conta que pode auxiliar os processos de consciencialização, os processos de responsabilização e controlo interno, os processos de percepção e reconhecimento do risco, bem como útil para apoio na tomada decisão

Com a elaboração deste trabalho, surgem algumas sugestões de trabalhos futuros, nomeadamente, a possibilidade de testar o modelo e *framework* apresentada em diferentes tipos de organizações, possibilitando analisar o seu comportamento e contributo em diferentes cenários.

8. Bibliografia

Caldeira, M., 2000. Critical Realism: A philosophical perspective for case study research in social sciences. *EPISTEM,* Volume 5-6, pp. 73-88.

Calder, A. & Watkins, S., 2008. *IT Governance A Manager´s Guide to Data Security and ISO 27001/ISO 27002, 4th edition.* s.l.:Kogan Page, ISBN 978 0 7494 5271 1.

CGTF, C. G. T. F. R., 2004. *Information Security Governance: A Call to Action, 2004,* USA: s.n.

Coelho, P., 2007. *Security Certification for organization: A framework to manage information security,* Lisboa: ISCTE.

Decreto Regulamentar n.º 60-A/2007, s.d. *Decreto Regulamentar n.º 60-A/2007.* s.l.:INCM.

Dhillon, G., 2006. *Principles of Information System Security: Text and Cases.* s.l.:s.n.

Earl, M. & Feeny, D., 2000. "How to be a CEO in the information age". *MIT Sloan Management Review,* Volume 41, p. 19.

ENISA Article 4, 2011. *Recommendations for the technical implementation of the Article 4 of the ePrivacy Directive,* s.l.: ENISA.

ENISA, 2012. *Framework de Gestão do Risco in ENISA http://www.enisa.europa.eu (acedido em 28/01/2012), 2012..* [Online]
Available at: http://www.enisa.europa.eu

Gillies, A., 2011. Improving the quality of information security management systems with ISO27000. *The TQM Journal,* Volume 23(4), pp. 367-376.

Guba, E. G. & Lincoln, Y. S., 1998. *Naturalistic and Rationalistic Enquiry. In Keeves, J.P.(Ed.), Educational Research, Methodology and Measurement: An International Handbook (pp. 81-85).* London: Pergamon Press.

ISO/IEC 13335-1, 2., 2004. *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management.* s.l.:s.n.

ISO/IEC 27000:2009, 2., 2009. *ISO/IEC 27000:2009— Information technology — Security techniques — Information security management systems — Overview and vocabulary ISO/IEC 27000:2009 (E).* s.l.:s.n.

ISO/IEC 27001:2005, 2., 2005. *ISO/IEC 27001:2005—A standard from the International Organization for Standardisation (ISO)/International Electrotechnical Commission (IEC) that covers all types of organizations.* s.l.:s.n.

ISO/IEC 27002:2005, 2., 2005. *ISO/IEC 27002:2005 : Information technology — Security techniques — Code of practice for information security management, ISO IEC.* s.l.:s.n.

ITSMF, 2011. *Maturidade da Governação e Gestão de TI em Portugal,* Lisboa: disponível em www.itsmf.pt.

Lapke, M. & Dhillon, G., 2008. *Power Relationships in Information Systems Security Policy Formulation and Implementation.* Galway, Ireland, s.n., pp. 1-12.

Macedo, B. A. R. d. S., 2009. *Um Modelo de Arquitectura de Sistemas de Informação,* s.l.: Universidade Técnica de Lisboa - Instituto Superior de Economia e Gestão.

Office, C., 2008. *Data Handling Procedures in Government: Final Report,* UK: Cabinet Office, disponivel em www.cabinetoffice.gov.uk.

Oliver, G., 2007. Implementing international standards: first, know your organisation. *Records Management Journal,* Volume 17(2), pp. 82 - 93.

Presidência do Conselho de Ministro, 2012. *Resolução do Conselho de Ministros n.º 12/2012.* s.l.:s.n.

Santos, A., 2007. *Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação,* Portugal: Universidade do Minho.

Serrano, A. M. S., Guerreiro, A. & Caldeira, M., 2004. *Gestão de sistemas e tecnologias de informação. 2ª ed. Lisboa.* Lisboa: FCA-Editora de Informática.

SGMOPTC Actividades, 2012. *SGMOPTC Plano de Actividades.* [Online]
Available at: http://www.sg.moptc.pt/tempfiles/20110303095341moptc.pdf

SGMOPTC Arquitectura, 2008. *Documento de politica de segurança e privacidade da SGMOPTC,* s.l.: s.n.

SGMOPTC Arquitectura, 2011. *Arquitectura de Sistemas de Informação,* Lisboa: MOPTC.

SGMOPTC, 2012. *Quadro de Avaliação e Responsabilização de 2011 (QUAR) da SGMOPTC.* [Online]
Available at: http://www.sg.moptc.pt/cs2.asp?idcat=2298

Siponen, M. & Willison, R., 2009. Information security management standards: Problems and solutions. *Information & Management,* Volume 46, pp. 267-270.

Smith, S., 2010. Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly,* Volume 34(3), pp. 463-486.

Straub, D. & Welke, R. J., 1998. Coping with Systems Risk: Security Planning Models for Management Decision-Making. *MIS Quarterly (22:4, December),* pp. pp. 441- 469.

Valdevit, T., Mayer, N. & Barafort, B., 2009. *Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings,* Luxembourg: OConnor RV.

Wright, S., 2006. *Measuring the Effectiveness of Security Using ISO 27001 Steve Wright,* UK: Siemens Insight Consulting.

Yin, R. K., 1994. *Case Study Research: Design and Methods (2nd Ed).* Thousand Oaks, CA: Sage Publications Inc.

9. Anexos

9.1.Anexo A – Mapa de controlos

MAPA DE CONTROLOS													
Cláusulas de controlo de segurança	**ID**	**Categorias**	**ID**	**Controlo Standard ISO/IEC 27002**	**Definição Controlo**	**Monitorização SGMOPTC 2011 Analise e Descrição**	**Nível de Classificação de Cumprimento**	**Nível de Exposição/Vulnerabilidade Nível de Cumprimento**	**Nível de Exposição/Vulnerabilidade com Cumprimento 1**	**Nível de Exposição/Vulnerabilidade com Cumprimento 1-2**	**Nível de Exposição/Vulnerabilidade com Cumprimento 3**	**Verificação de responsabilidade**	**Observações**
Política de Segurança	**5.1**	**Política de Segurança da Informação**	**5.1.1**	Documento da política segurança da informação	Um documento de política de segurança da informação deve ser aprovado pela gestão, publicado e comunicado a todos os empregados e partes externas relevantes	Existe uma versão de 16 de Junho 2008 do documento de Política de Segurança, não aprovado pela gestão.	2	1		1		Gestão de topo; DSTIC	Sugere-se validação/revisão das conformidades do documento
	5.1		**5.1.2**	Documento da política segurança da informação	A política de segurança da informação deve ser revista em intervalos planeados ou quando ocorrerem mudanças significativas, de modo a assegurar a sua contínua pertinência, adequação e eficácia	Não existe plano de revisão estabelecido. Existe proposta de revisão em curso para 2011	2	1		1		DSTIC	Definição de planos de implementação e revisão periódica dos documentos com atribuição de responsabilidades. Anexa ao documento de política de segurança da informação
Organização da Segurança	**6.1**	**Organização interna**	**6.1.1**	Comprometimento da gestão com a segurança da informação	A gestão deve apoiar activamente a segurança dentro da organização por meio de uma clara orientação, demonstrando o seu comprometimento, definindo atribuições de forma explícita e reconhecendo as responsabilidades pela segurança da informação.	Existe comprometimento verbal da gestão	2	1	1	1		Gestão de topo	
	6.1		**6.1.2**	Coordenação da segurança da informação	As actividades de segurança da informação devem ser coordenadas por representantes de diferentes partes da organização, com funções e responsabilidades relevantes.	Não existe plano definido, existe uma versão de 16 de Junho 2008 do documento de Política de Segurança	1	2	2	2		Gestão de topo; DSTIC	
	6.1		**6.1.3**	Atribuição de responsabilidades de segurança da informação	Todas as responsabilidades pela segurança da informação devem estar definidas de forma clara.	Não existe plano de responsabilidades definido	2	2		2		DSTIC	
	6.1		**6.1.4**	Processo de autorização para os recursos de processamento de informação	Deve ser definido e implementado um processo de gestão de autorização para novos recursos de processamento de informação.	Não existe plano de autorização	1	1	1	1		DSTIC	
	6.1		**6.1.5**	Acordos de confidencialidade	Devem ser identificados e revistos, de forma regular, os requisitos para os acordos de	Não existe plano definido	1	2	2	2		DSTIC	

					confidencialidade ou de não divulgação de informação, de modo que estes reflictam as necessidades da organização para a protecção da informação.								
	6.1		**6.1.6**	Contacto com autoridades públicas	Devem ser mantidos contactos apropriados com as autoridades públicas relevantes.	Pouca participação	1	1	1	1		Gestão de topo; DSTIC	
	6.1		**6.1.7**	Contacto com grupos de interesse especial	Devem ser mantidos contratos apropriados com grupos de interesse especial ou outros fóruns especializados em segurança da informação e associações profissionais	Alguma participação	1	1	1	1		Gestão de topo; DSTIC	
	6.1		**6.1.8**	Revisão independente de segurança da informação	A abordagem da organização para gerir a segurança da informação e a sua implementação (ou seja os objectivo dos controlos, controlos, políticas, processos e procedimentos para a segurança da informação) deve ser revista, de forma independente, em intervalos planeados, ou quando ocorrerem mudanças significativas para a implementação de segurança.	Abordagem independente sem plano prévio estabelecido	3	1				DSTIC	Os planos e equipas para a realização de análises e auditorias aos sistemas de informação devem constar de planos periódicos de implementação com definição de equipas de trabalho previamente estabelecidos e aprovados
	6.2	**Partes externas**	**6.2.1**	Identificação dos riscos relacionados com partes externas	Os riscos, para a informação e para os recursos de processamento de informação da organização, decorrentes de processos do negócio que envolvam partes externas devem ser identificados e devem ser implementados controlos apropriados antes de se conceder o acesso.	Não existe levantamento e controlos estabelecidos	1	3	3	3		DSTIC	Importante estabelecer plano e controlos conjuntamente com a Politica de Segurança
	6.2		**6.2.2**	Endereçar a segurança da informação quando lidar com clientes.	Todos os requisitos identificados de segurança da informação devem ser considerados antes de conceder aos clientes o acesso aos activos ou às informações da organização.	Existe precaução do estabelecimento do acesso sem definição previa dos requisitos	2	3		3		DSTIC	Plano de requisitos
	6.2		**6.2.3**	Endereçar a segurança da informação nos acordos com terceiras partes	Os acordos com terceiras partes, que envolvam o acesso, processamento, comunicação ou a gestão da informação ou dos recursos de processamento de informação da organização, bem	Existe precaução do estabelecimento do acesso com as partes sem definição previa dos requisitos	2	3		3		DSTIC	Plano de requisitos

					como o acréscimo de produtos ou serviços aos recursos de processamento de informação, devem cobrir todos os requisitos de segurança da informação relevantes.								
Gestão de Activos	**7.1**	**Responsabilidade pelos activos**	**7.1.1**	Inventário de activos	Todos os activos devem ser identificados de forma clara. Um inventário, de todos os activos importantes, deve ser estruturado e mantido.	Existe cadastro de activos	3	1			1	DSTIC; DRP	DRP - Plano de inventário
	7.1		**7.1.2**	Responsabilidade pelos activos	Todas as informações e activos associados com os recursos de processamento de informação devem ter um responsável designado por uma parte definida da organização	Não existe responsável formal directo estabelecido	1	1	1	1		DSTIC; DRP	DSTIC - Tabela de atribuição de responsabilidades
	7.1		**7.1.3**	Utilização aceitável dos activos	Devem ser identificadas, documentadas e implementadas regras para a utilização aceitável de informações e dos activos associados aos recursos de processamento de informação	Não existem regras prévias definidas	1	1	1	1		DSTIC; DRP	DSTIC ; DRP documentação
	7.2	**Classificação da Informação**	**7.2.1**	Directrizes de classificação	A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e grau de importância para a organização.	A classificação formal não é usada	2	2		2		DSTIC; DRP	DSTIC ; DRP documentação
	7.2		**7.2.2**	Etiquetagem e manuseamento de informação	Um conjunto apropriado de procedimentos para etiquetar e manusear a informação deve ser definido e implementado de acordo com o esquema de classificação adoptado pela organização	Existe etiquetagem sem regras prévias formais	2	2		2		DSTIC; DRP	DSTIC ; DRP documentação e etiquetagem

Fonte: Estudo de caso SGMOPTC – Mapa de Controlos (excerto)

Figura 9-1 Mapa de controlos

9.2.Anexo B - Mapa de classificação de cumprimento

Nível de classificação de cumprimento por clausulas e categoria						
Nº	**Cláusula**	**Categoria**	**Controlo**	**Nível de Classificação de Cumprimento**	**Média por cláusula**	**Média por categoria**
1	5	5.1	5.1.1	2		
2	5		5.1.2	2	2,00	2,00
3	6	6.1	6.1.1	2		
4	6		6.1.2	1		
5	6		6.1.3	2		
6	6		6.1.4	1		
7	6		6.1.5	1		
8	6		6.1.6	1		
9	6		6.1.7	1		
10	6		6.1.8	3		1,50
11	6	6.2	6.2.1	1		
12	6		6.2.2	2		
13	6		6.2.3	2	1,55	1,67
14	7	7.1	7.1.1	3		
15	7		7.1.2	1		
16	7		7.1.3	1		1,67
17	7	7.2	7.2.1	2		
18	7		7.2.2	2	1,80	2,00
19	8	8.1	8.1.1	1		
20	8		8.1.2	1		
21	8		8.1.3	1		1,00
22	8	8.2	8.2.1	1		
23	8		8.2.2	1		
24	8		8.2.3	1		1,00
25	8	8.3	8.3.1	2		
26	8		8.3.2	3		
27	8		8.3.3	3	1,56	2,67
28	9	9.1	9.1.1	3		
29	9		9.1.2	3		
30	9		9.1.3	2		
31	9		9.1.4	2		
32	9		9.1.5	2		
33	9		9.1.6	3		2,50
34	9	9.2	9.2.1	3		
35	9		9.2.2	3		
36	9		9.2.3	3		
37	9		9.2.4	3		
38	9		9.2.5	2		
39	9		9.2.6	2		
40	9		9.2.7	3	2,62	2,71
41	10	10.1	10.1.1	2		
42	10		10.1.2	1		
43	10		10.1.3	2		
44	10		10.1.4	3		2,00
45	10	10.2	10.2.1	2		
46	10		10.2.2	3		
47	10		10.2.3	1		2,00
48	10	10.3	10.3.1	2		
49	10		10.3.2	3		2,50
50	10	10.4	10.4.1	2		
51	10		10.4.2			2,00
52	10	10.5	10.5.1	3		3,00
53	10	10.6	10.6.1	3		
54	10		10.6.2	3		3,00
55	10	10.7	10.7.1	2		
56	10		10.7.2	3		
57	10		10.7.3	3		
58	10		10.7.4	3		2,75
59	10	10.8	10.8.1	1		
60	10		10.8.2	2		
61	10		10.8.3	2		
62	10		10.8.4	3		
63	10		10.8.5	1		1,80
64	10	10.9	10.9.1	3		

Fonte: Estudo de caso SGMOPTC – Mapa de Controlos (excerto)

Figura 9-2 Mapa de classificação de cumprimento – cláusulas e categorias

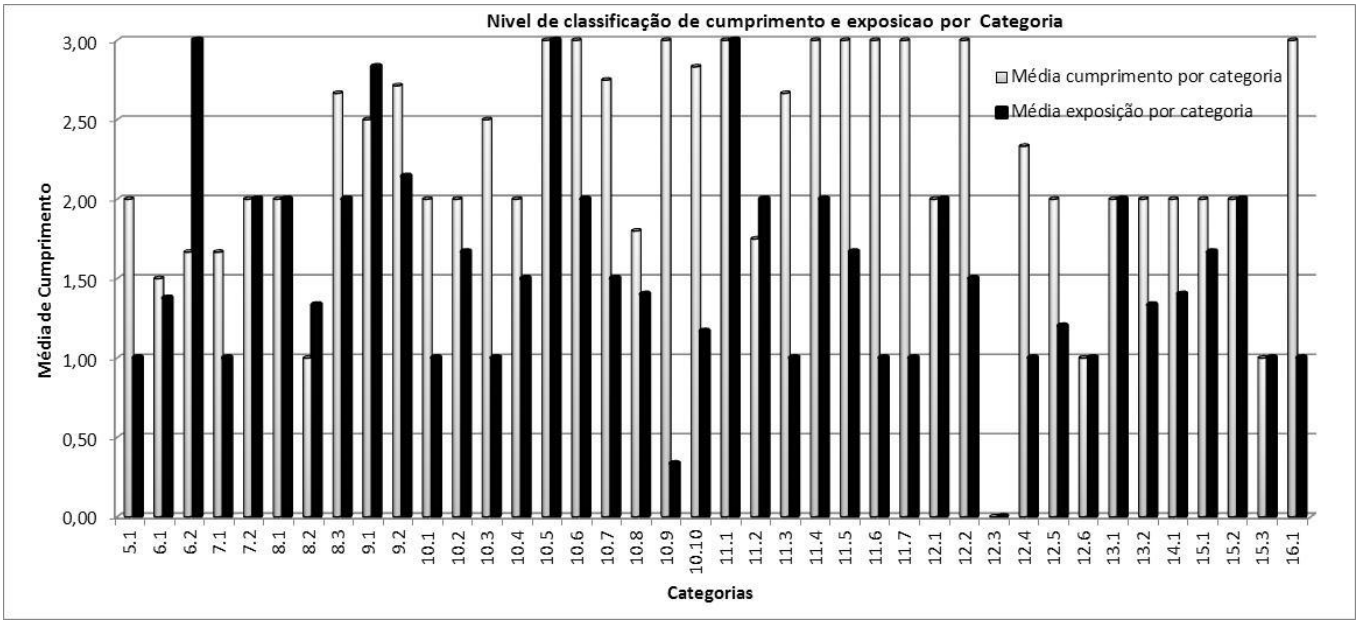
9.3.Anexo C – Matriz de controlo e definição de responsabilidades

MATRIZ DE CONTROLO E DEFINIÇÃO DE RESPONSABILIDADES				
Controlo	**UO Área de Responsabilidade**	**ID Área**	**Média de classificação de cumprimento da Categoria**	**Objectivo/Meta Categoria**
5.1.1	Gestão de topo; DSTIC	9	2,00	Proporcionar uma orientação e apoio da gestão para a segurança da informação de acordo com os requisitos de negócio e com as leis e regulamentações aplicáveis.
5.1.2	DSTIC	1		
6.1.1	Gestão de topo	8	1,50	Gerir a segurança da informação na organização.
6.1.2	Gestão de topo; DSTIC	9		
6.1.3	DSTIC	1		
6.1.4	DSTIC	1		
6.1.5	DSTIC	1		
6.1.6	Gestão de topo; DSTIC	9		
6.1.7	Gestão de topo; DSTIC	9		
6.1.8	DSTIC	1		
6.2.1	DSTIC	1	1,67	Manter a segurança da informação e dos recursos de processamento de informação da organização, que são acedidos, processados, comunicados, ou geridos por partes externas.
6.2.2	DSTIC	1		
6.2.3	DSTIC	1		
7.1.1	DSTIC; DRP	7	1,67	Alcançar e manter a protecção adequada dos activos da organização.
7.1.2	DSTIC; DRP	7		
7.1.3	DSTIC; DRP	7		
7.2.1	DSTIC; DRP	7	2	Assegurar que a informação obtém um nível adequado de protecção.
7.2.2	DSTIC; DRP	7		
8.1.1	DSTIC; DRH	4	1	Assegurar que os empregados, fornecedores e utilizadores de terceiras partes compreendam as suas responsabilidades, e que sejam adequados para o desempenho das funções para as quais estão a ser considerados, e reduzir o risco de roubo, fraude ou utilização indevida de recursos. [1]. A expressão "prestação laboral" pretende cobrir as seguintes diferentes situações: o emprego de pessoas (temporário ou sem termo), a nomeação para cargos, as mudanças de cargos, a assinatura de contratos e o término de qualquer das relações jurídicas mencionadas. [Na versão em língua inglesa é empregue o termo "employment"]
8.1.2	DSTIC; DRH	4		
8.1.3	DSTIC; DRH	4		
8.2.1	Gestão de topo	8	1	Assegurar que todos os empregados, fornecedores e utilizadores de terceiras partes estão conscientes das ameaças e preocupações relativas à segurança da informação, bem como das suas responsabilidades e obrigações legais, e que estão preparados para apoiar a política de segurança da informação da organização no âmbito dos seus trabalhos e de forma a reduzir o risco de erro humano.
8.2.2	DSTIC; DRH; Gestão de Topo	5		
8.2.3	DSTIC; DRH; Gestão de Topo	5		
8.3.1	DSTIC; DRH; Gestão de Topo	5	2,67	Assegurar que empregados, fornecedores e utilizadores de terceiras partes deixem a organização ou alterem o seu trabalho de forma ordenada.
8.3.2	DSTIC; DRP	7		
8.3.3	DSTIC; SAP	3		
9.1.1	DSTIC; DRP	7	2,5	Prevenir o acesso físico não autorizado, danos e interferências nas instalações e nas informações da organização.
9.1.2	DSTIC	1		
9.1.3	DSTIC; DRP	7		
9.1.4	DSTIC; DRP	7		
9.1.5	DSTIC; DRP	7		
9.1.6	DSTIC; DRP	7		
9.2.1	DSTIC; DRP	7	2,71	Prevenir a perda, o dano, o furto ou o comprometimento de activos e a interrupção das actividades da organização.
9.2.2	DSTIC; DRP	7		
9.2.3	DSTIC; DRP	7		
9.2.4	DSTIC	1		
9.2.5	DSTIC; DRP	7		
9.2.6	DSTIC	1		
9.2.7	DSTIC; DRP	2		
10.1.1	DSTIC	1	2	Garantir a operação correcta e segura dos recursos de processamento de informação.
10.1.2	DSTIC	1		
10.1.3	DSTIC	1		
10.1.4	DSTIC	1		
10.2.1	DSTIC	1	2	Implementar e manter o nível apropriado de segurança da informação e de disponibilização de serviços de acordo com contratos de prestação de serviço de terceiras partes.
10.2.2	DSTIC	1		
10.2.3	DSTIC	1		
10.3.1	DSTIC	1	2,5	Minimizar o risco de falhas dos sistemas.
10.3.2	DSTIC	1		
10.4.1	DSTIC	1	2	Proteger a integridade do software e da informação.
10.4.2	DSTIC	1		
10.5.1	DSTIC	1	3	Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.
10.6.1	DSTIC	1	3	Garantir a protecção das informações nas redes e a protecção da infra-estrutura de suporte.
10.6.2	DSTIC	1		
10.7.1	DSTIC	1	2,75	Prevenir contra a divulgação não autorizada, modificação, remoção ou destruição dos activos, e interrupções nas actividades de negócio.
10.7.2	DSTIC	1		
10.7.3	DSTIC	1		
10.7.4	DSTIC	1		

Fonte: Estudo de caso SGMOPTC – Mapa de Controlos (excerto)

Figura 9-3 Matriz de controlo e definição de responsabilidades

9.4.Anexo D – Gráfico de classificação de cumprimento e exposição



Fonte: Estudo de caso SGMOPTC – Mapa de Controlos

Figura 9-4 Gráfico de classificação de cumprimento e exposição

9.5.Anexo E – Funções de negócio/unidades orgânicas SGMOPTC

Direcção de Serviços	**Serviço prestado**
Direcção de Serviços de Administração de Recursos	Gestão Financeira e Orçamental; Recursos Humanos
Direcção de Serviços de Tecnologias de Informação e Comunicações	Gestão de Tecnologias de Informação e Comunicações
Direcção de Serviços Jurídicos e Contencioso	Gestão Administrativa, Legislativa e Apoio Técnico
Direcção de Serviços de Documentação, Informação e Comunicação	Informação e Documentação
Unidade Ministerial de Compras	Gestão de Bens, Aprovisionamento e Aquisição de Bens e Serviços

Fonte: Adaptado de (SGMOPTC Actividades, 2012)

Tabela 9-1 Unidades orgânicas e serviços prestados

9.6.Anexo F – Listagem de clientes SGMOPTC

Clientes		
GabLogis	Gabinete Para o Desenvolvimento do Sistema Logístico Nacional	Administração Directa do Estado:
GMOPTC	Gabinete do Ministro das Obras Públicas, Transportes e Comunicações	
GSEAOPC	Gabinete do Secretário de Estado Adjunto das Obras Públicas e Comunicações	
GSET	Gabinete do Secretário de Estado dos Transportes	
GPERI	Gabinete de Planeamento, Estratégia e Relações Internacionais	
IGOPTC	Inspecção-Geral das Obras Públicas, Transportes e Comunicações	
GPIAA	Gabinete de Prevenção e Investigação de Acidentes com Aeronaves	
GISAF	Gabinete de Investigação de Segurança e de Acidentes Ferroviários	
POVT	Programa Operacional Temático de Valorização do Território	
CPETA	Comissão de Planeamento e Emergência do Transporte Aéreo	
CPETT	Comissão de Planeamento e Emergência do Transporte Terrestre	
CPTM	Comissão de Planeamento e Emergência do Transporte Marítimo	
IMTT	Instituto da Mobilidade e dos Transportes Terrestres	
INIR	Instituto de Infra-estruturas Rodoviárias	Administração Indirecta do Estado:
IPTM	Instituto Portuário e dos Transportes Marítimos	
INAC	Instituto Nacional de Aviação Civil	
INCI	Instituto da Construção e do Imobiliário	
LNEC	Laboratório Nacional de Engenharia Civil	
FSI	Fundo para a Sociedade de Informação	

Fonte: Adaptado de (SGMOPTC Actividades, 2011)

Tabela 9-2 Listagem de clientes SGMOPTC

9.7.Anexo G – Cláusulas de controlo de segurança

Controlo	Cláusulas de controlo de segurança
A.5	Política de segurança
A.6	Organização da segurança da informação
A.7	Gestão de activos
A.8	Segurança de recursos humanos
A.9	Segurança física e ambiental
A.10	Gestão das operações e comunicações
A.11	Controlo de acessos
A.12	Aquisição, desenvolvimento e manutenção de sistemas de informação
A.13	Gestão de incidentes de segurança da informação
A.14	Gestão da continuidade de negócio
A.15	Conformidade
A.16	Gestão de incidentes

Fonte: Adaptado de (ISO/IEC 27002:2005, 2005)

Tabela 9-3 Clausulas de controlo de segurança